

Почему не работает WiFi



Solution.
Production.
Warranty.



официальный дистрибутор

www.spw.ru

Об авторе

- Илья Князев. г. Санкт-Петербург, Россия.
- Mikrotik Certified Trainer [TR0309]
- МТСНА, МТСТСЕ, МТСВЕ, МТСУМЕ, МТСРЕ, МТСИНЕ, МТСIPv6Е
- Технический директор SPW.RU

Координаты для связи

- E-Mail: ikn@spw.ru
- Skype: Ilya.Knyazev
- WWW: <https://spw.ru>

Введение

- Беспроводные сети прочно вошли в нашу жизнь.
- Без существенных усилий можно найти много литературы по их настройке и обслуживанию
- Тем не менее они не всегда работают так, как нам того хочется

Причины плохой работы

- Плохое проектирование сети
- Плохая настройка точек доступа
- Изменение радиообстановки
- Целенаправленная атака на вашу сеть

Как найти причину?

- Для поиска причины плохой работы беспроводной сети требуется использование специализированного программного обеспечения и оборудования
- Кроме того потребуются
 - Знания
 - Терпение
 - Время

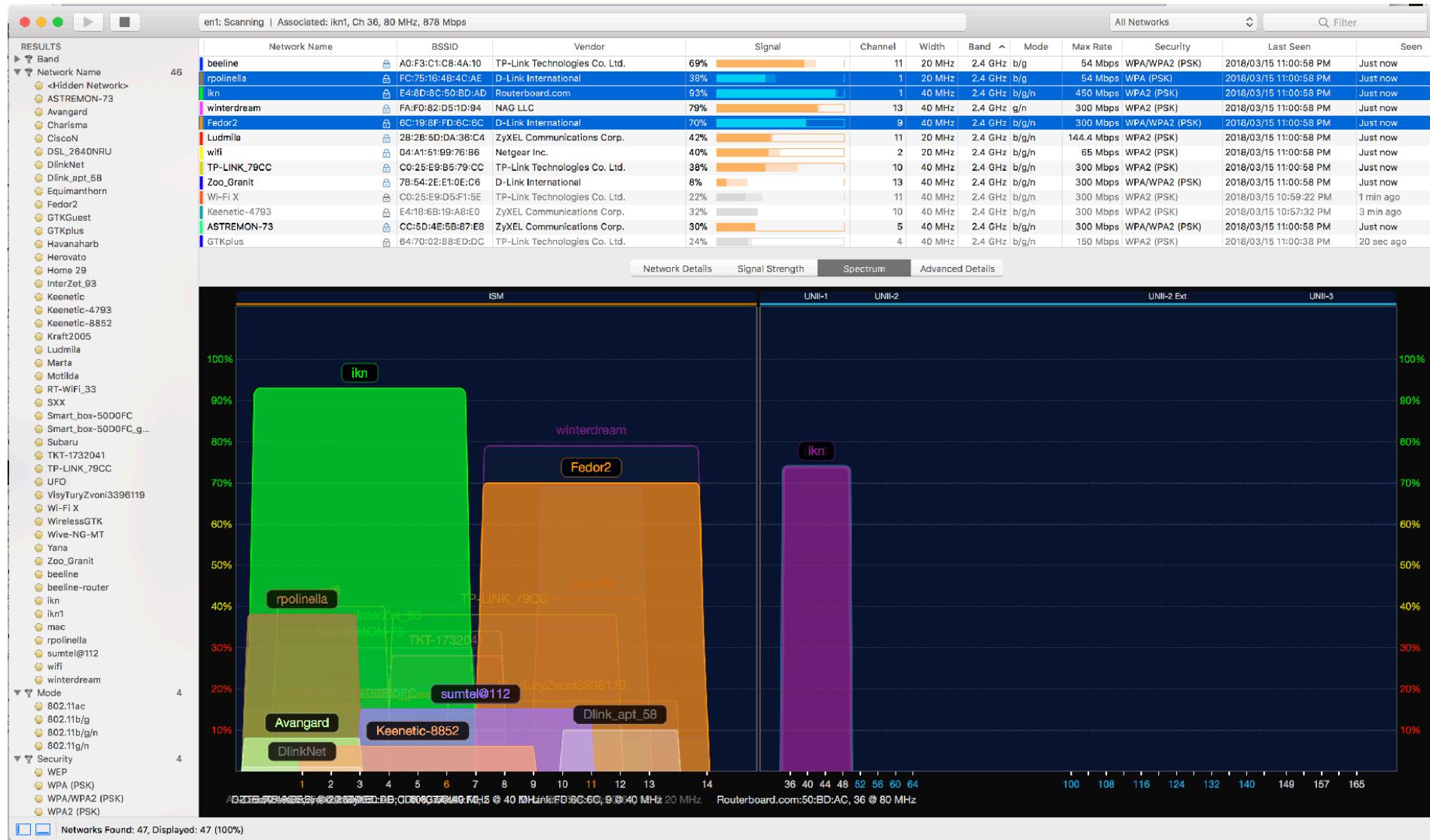
Программы которые помогут

- Самый простой и распространенный класс программ это Wi-Fi сканеры.
- Они обладают не самым выдающимся функционалом, но зато просты в эксплуатации, дешевы или вообще бесплатны
- Типичные примеры:
Inssider, Wireless Explorer и т.п.

WiFi-сканнер

- Типичный функционал
- Сканирование эфира на наличие сетей, их распределения по каналам, вывод дополнительной информации по сетям
- Мониторинг уровня сигнала
- Выдача информации в удобном графическом виде

WiFi-Сканер



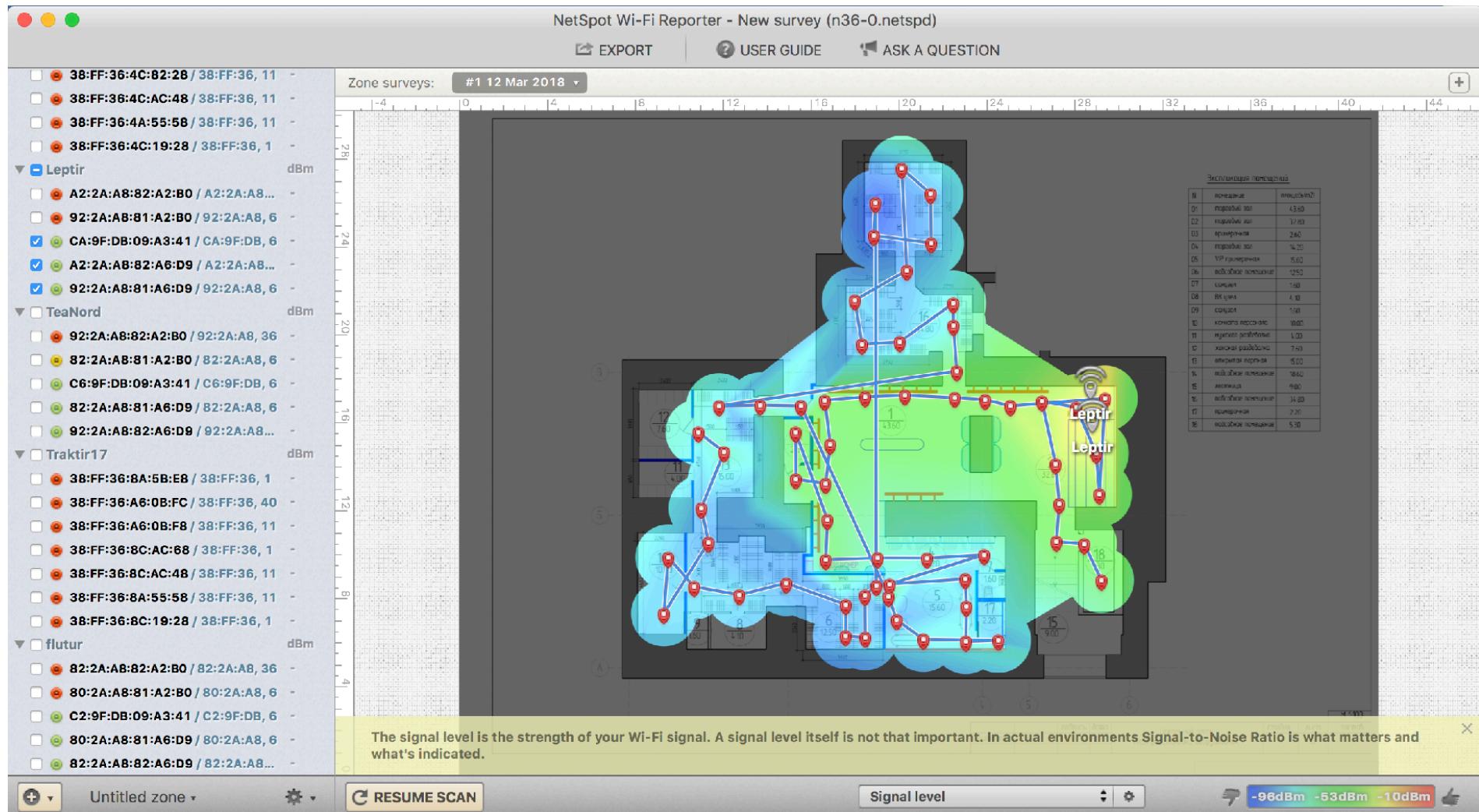
WiFi-Сканер

- Минусы этих программ
- Невысокий функционал
- Отсутствие привязки уровня сигнала к карте объекта
- Сканируется только WiFi. То есть только то, что «видит» драйвер радиокарты вашего устройства

WiFi Survey

- Следующий по сложности класс программ
- Позволяет построить карту покрытия помещения с визуализацией
- Находит и показывает на плане примерное расположение точек доступа
- Позволяет посмотреть как покрытие каждой отдельной точки доступа, так и всей сети в целом
- Типичные представители:
Ekahau, NetSpot и другие

WiFi Survey



WiFi-Survey

- Недостатки этого класса программ
- Как правило не бесплатны
- Требуют наличия плана помещения и привязки масштаба
- Так же как и предыдущее ПО могут анализировать только ту информацию, которую выдал драйвер радиокарты

Спектроанализаторы

- Либо отдельное устройство, либо программно-аппаратный комплекс
- Имеют очень высокий функционал для изучения эфира
- Не ограничены возможностями сетевой карты ПК
- Могут помочь в сложных случаях
- Могут использоваться для лабораторных исследований

Спектроанализаторы



RF-Explorer Combo



Oscium



Rohde and Schwarz FSH828

Встроенные инструменты RouterOS

- Mikrotik RouterOS имеет много полезных инструментов для анализа беспроводной сети
- Это встроенные в RouterOS
Wireless Scan
Wireless Snooper
Spectral Scaner
Wireless Sniffer
- И отличный Spectral-Scaner входящий в The Dude!

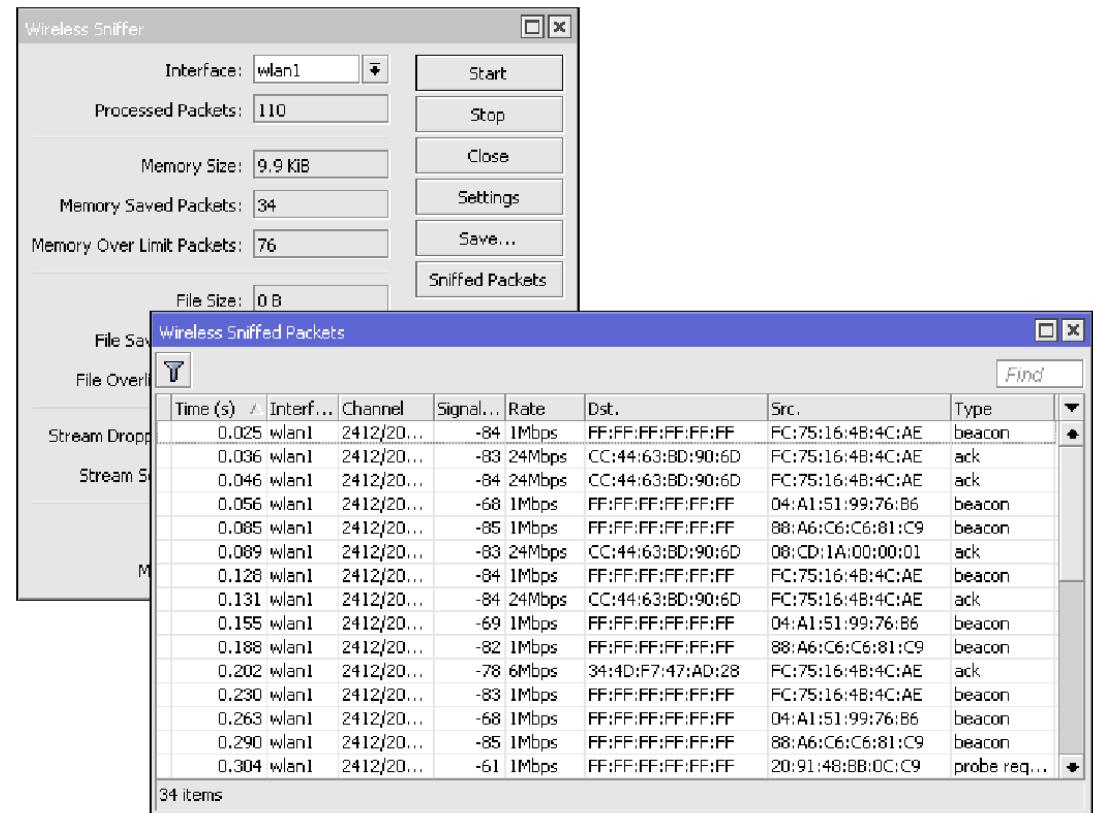
Wireless Snooper

- Покажет вам все WiFi-устройства которые найдет в эфире ваш маршрутизатор
- Все сети, процент использования частот, количество станций на каждом канале

Wireless Snooper (Running)									
Interface: wlan1									
Channel	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net... Sta...	all	▼
2412/2...	88:A6:C6:81:C9	RT-WIFI_33		2.7	39.6	25.9 kbps	1		▲
2412/2...	FC:75:16:4B:4C:AE	rpolinella		1.7	24.7	15.4 kbps	1		▼
2412/2...	88:A6:C6:81:C9	RT-WIFI_33	-86	2.7	39.6	25.9 kbps			▲
2412/2...	FC:75:16:4B:4C:AE	rpolinella	-83	1.7	24.7	15.4 kbps			▼
2412/2...	A8:72:30:00:CB:00			-75	0.0	0.0	0 bps		▲
2412/2...	72:65:70:6C:79:0E			-82	0.0	0.0	0 bps		▼
2412/2...				7.0		52.8 kbps	2 4		▲
2417/2...	04:A1:51:99:76:B6	wifi		2.4	37.4	22.2 kbps	2		▼
2417/2...	F8:F0:82:62:B9:E8	InterZet_93		1.0	15.6	9.1 kbps	1		▲
2417/2...	04:A1:51:99:76:B6	wifi		-67	2.4	22.2 kbps			▼
2417/2...	F8:F0:82:62:B9:E8	InterZet_93	-90	1.0	15.6	9.1 kbps			▲
2417/2...	00:00:81:00:00:00			-59	0.0	0.0	0 bps		▼
2417/2...	B0:70:2D:43:D1:0D	wifi		-63	0.0	0.0	0 bps		▲
2417/2...	00:00:88:01:00:02			-89	0.0	0.0	0 bps		▼
2417/2...				6.4		51.2 kbps	2 5		▲
2422/2...	CC:71:30:00:CB:00			-55	0.0	0.0	0 bps		▼
2422/2...				2.4		22.5 kbps	0 1		▲
2427/2...	64:70:02:88:ED:DC	GTKplus		0.0	0.0	0 bps			▼
2427/2...	20:91:48:BB:0C:C9			-55	0.0	0.0	0 bps		▲
2427/2...	EC:10:78:16:C6:BB			-69	0.0	0.0	0 bps		▼
2427/2...	64:70:02:88:ED:DC	GTKplus	-88	0.0	0.0	0 bps			▲
2432/2...	FA:F0:82:56:E5:2C	SXX		0.0		0 bps	1 3		▼
2432/2...	FA:F0:82:CD:0A:08	olga		1.6	100.0	14.6 kbps	1		▲
2432/2...				0.0	0.0	0 bps	1		▼
58 items									

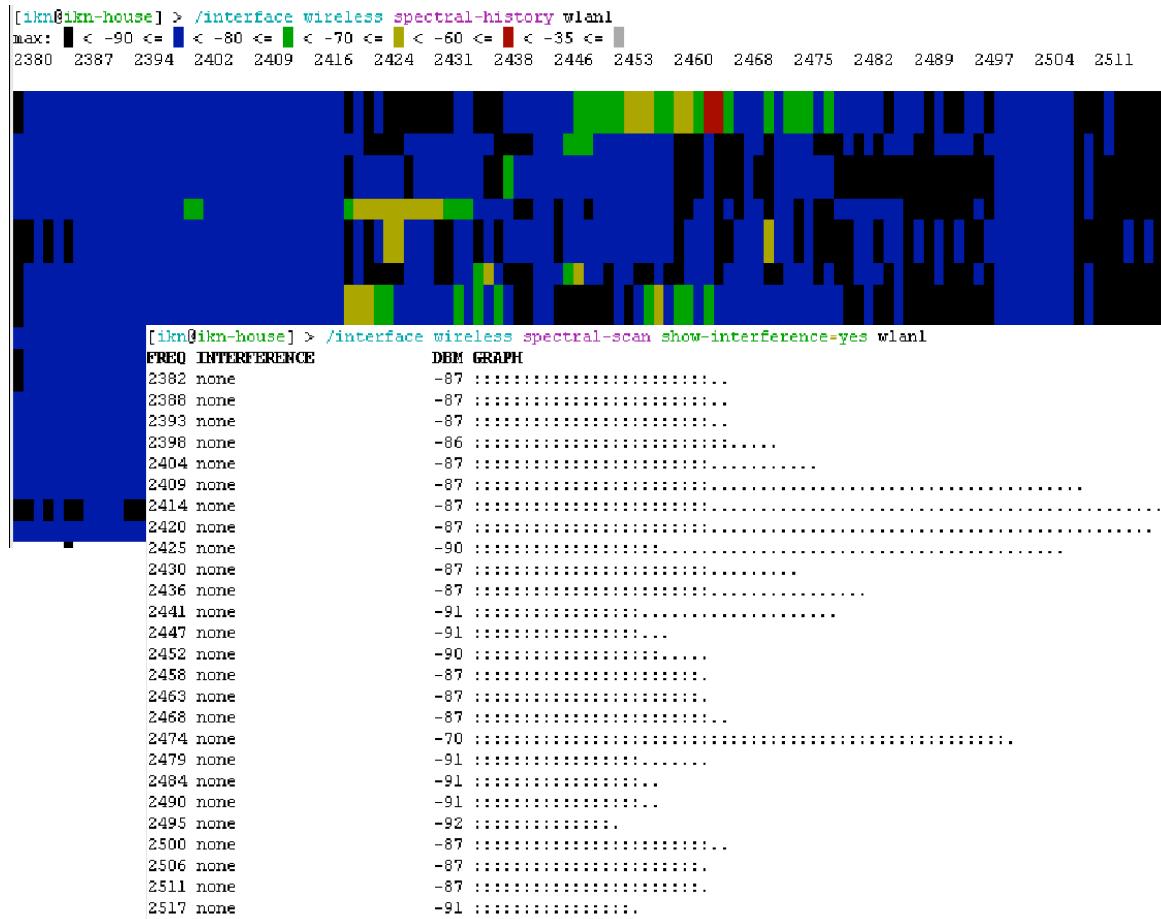
Wireless Sniffer

- Позволит вам проанализировать какие данные передаются в эфире
- Незаменимая вещь при обнаружении атаки на деаутентификацию



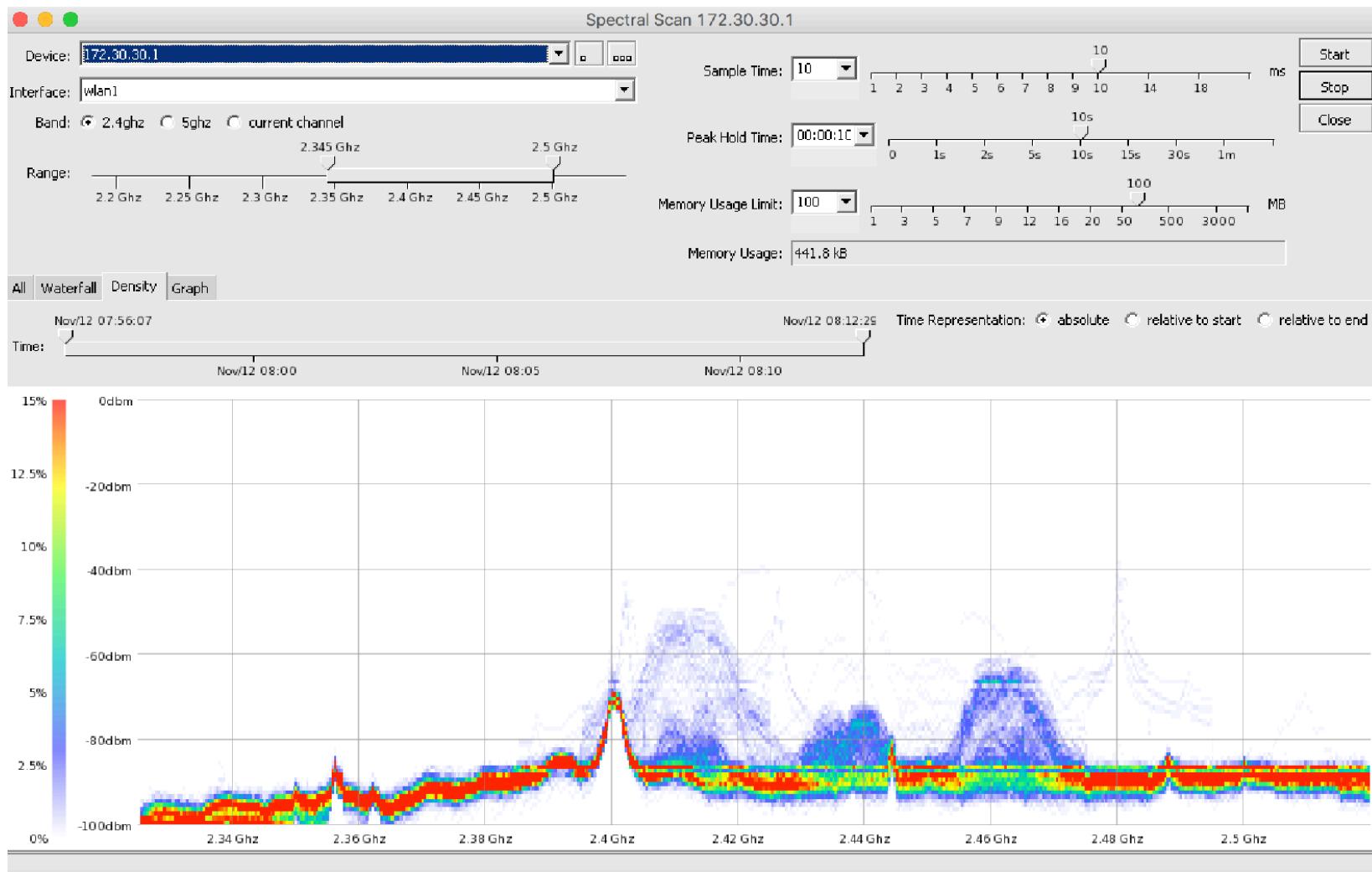
Spectral Scan

- Покажет
МОЩНОСТЬ
излучения и
известные
помехи

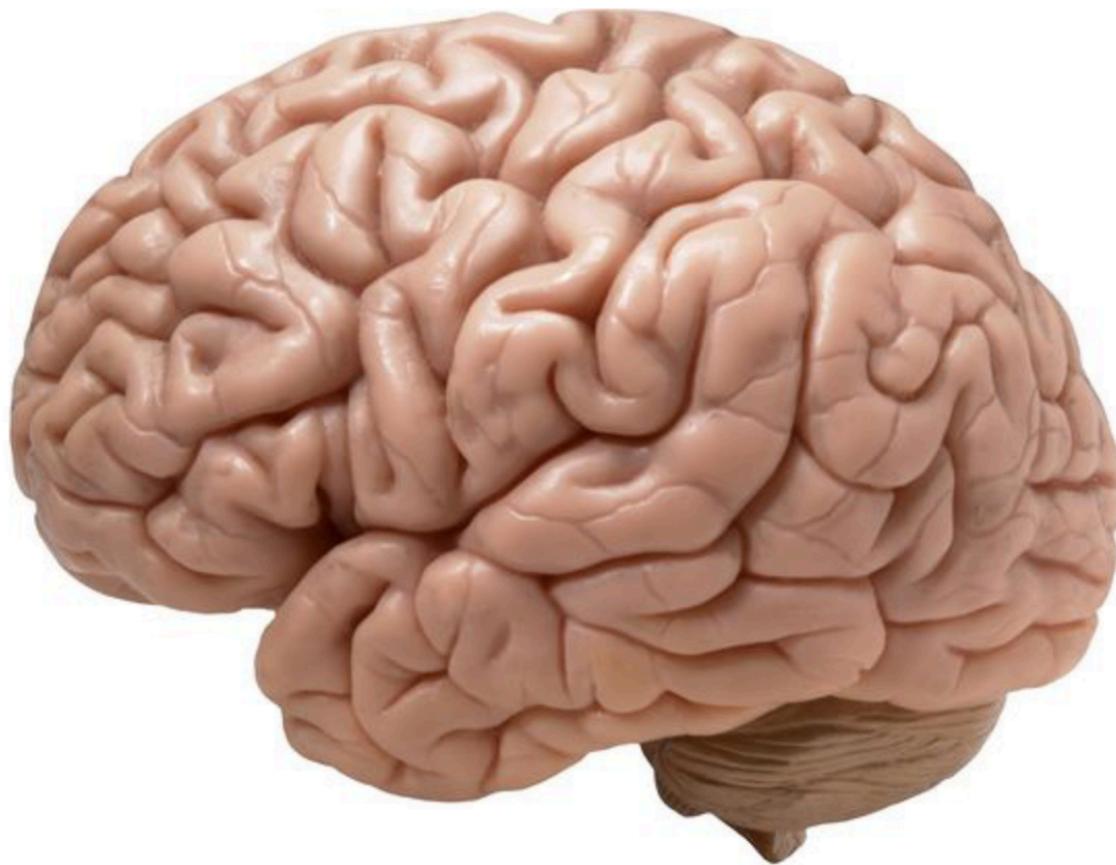


The Dude!

- В Mikrotik Dude есть отличная реализация спектрального анализатора

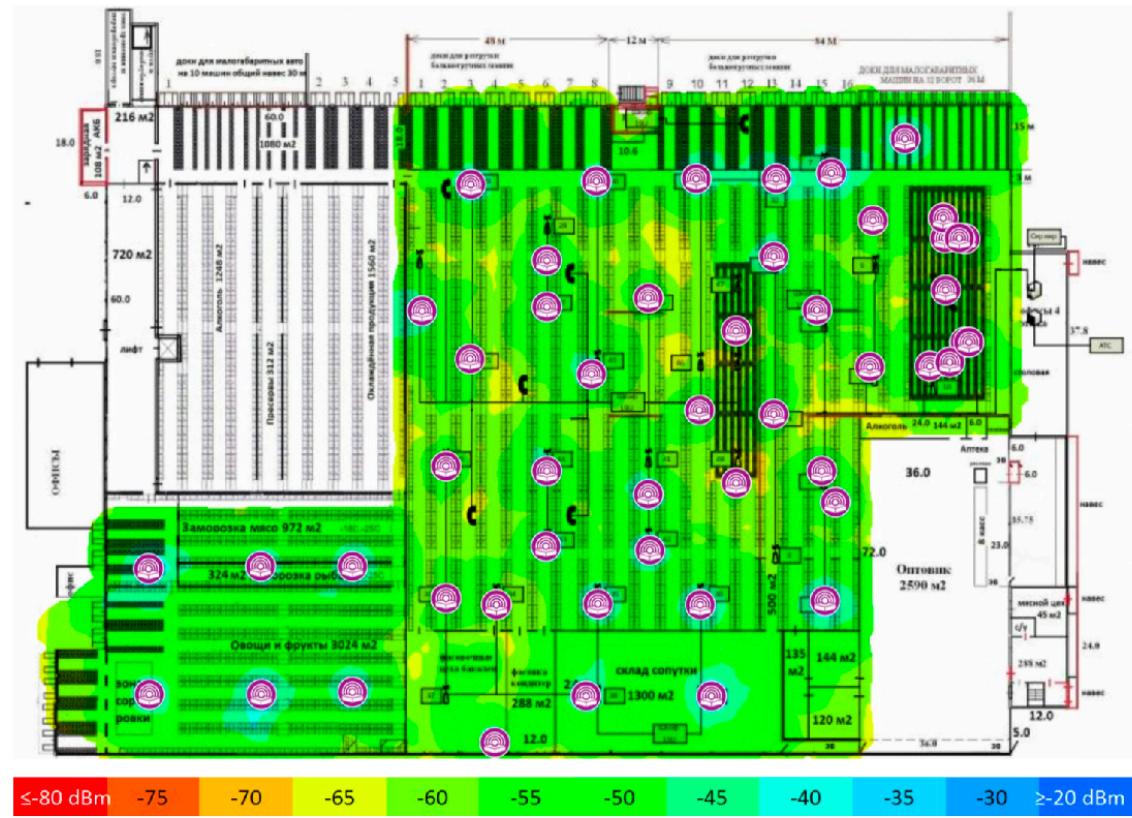


Самый главный инструмент



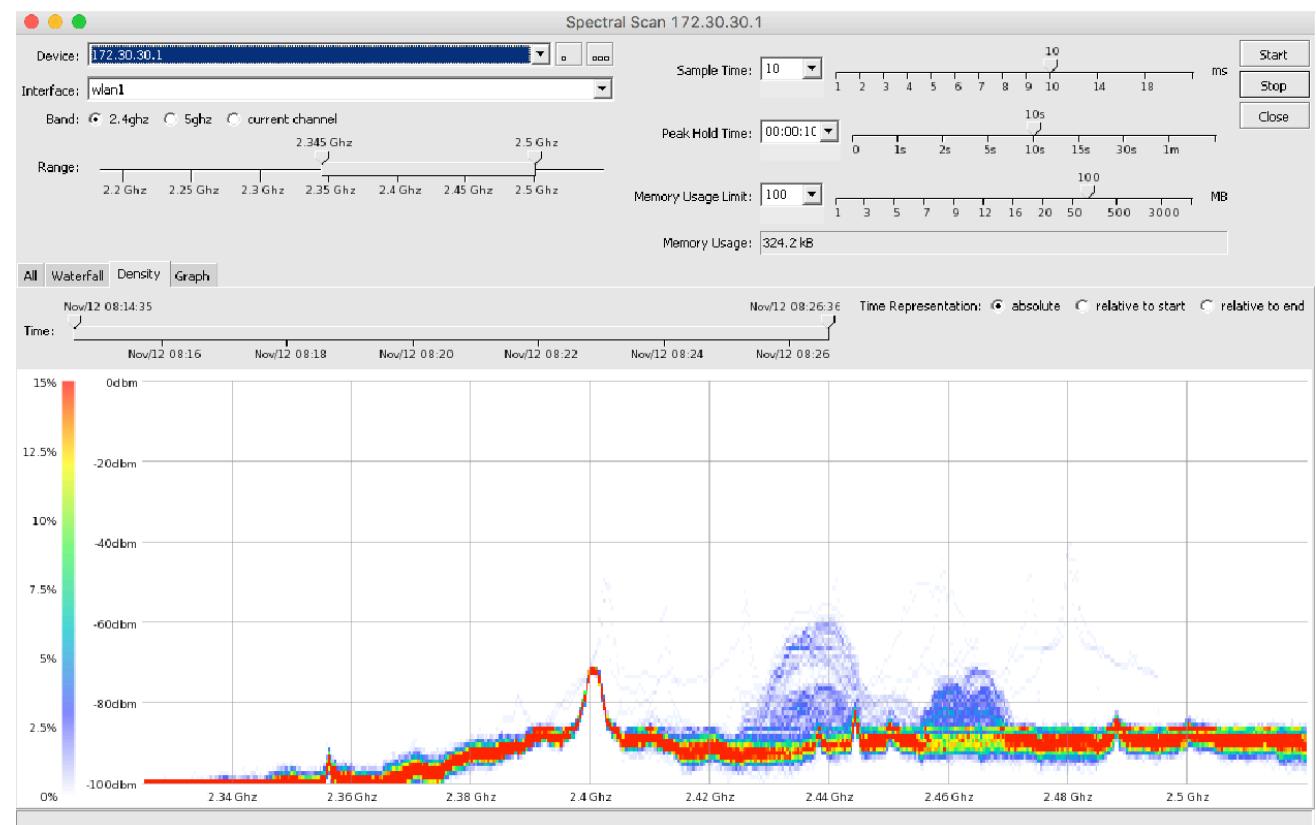
Пример поиска проблемы

- Жалобы на нестабильную работу WiFi
- Клиент самостоятельно произвел работы по визуализации покрытия
- Покрытие выглядит хорошо



Пример поиска проблемы

- Выезжаем на объект
- Запускаем Spectral Scan в the Dude
- Картинка близка к идеальной



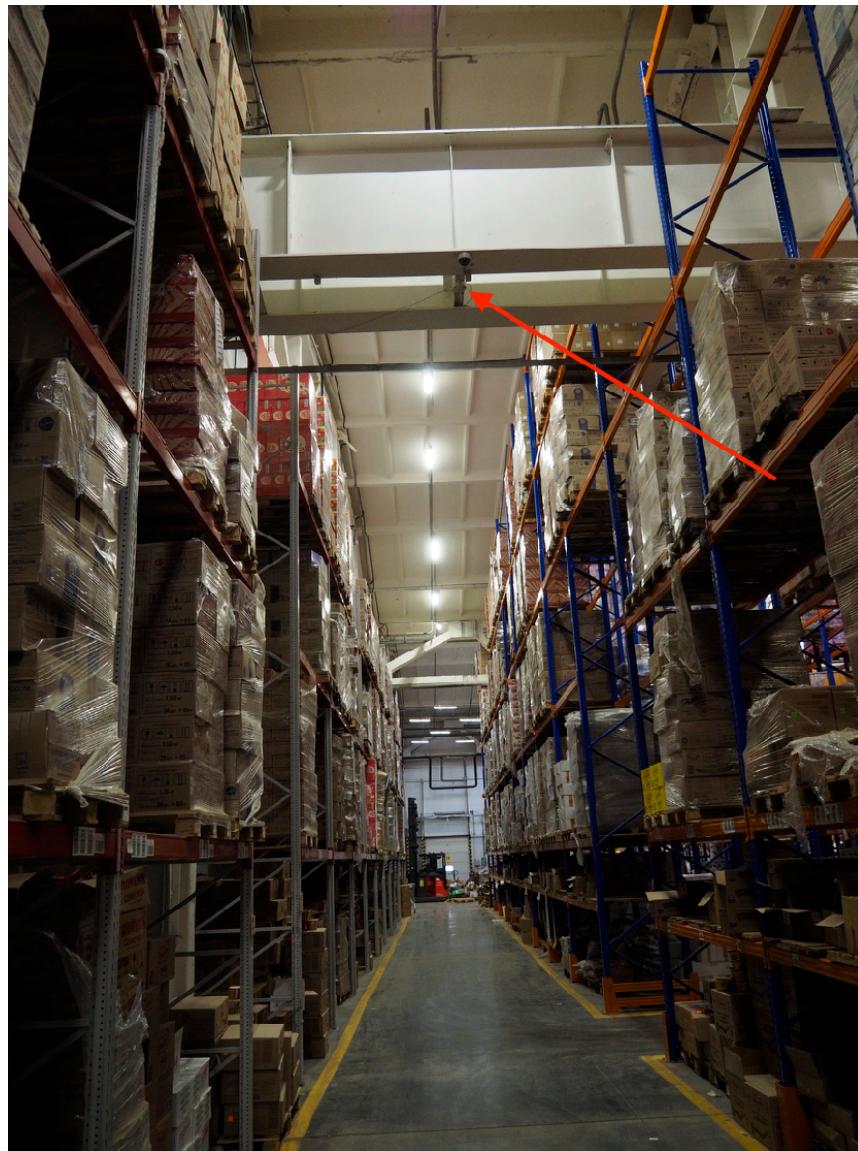
Пример поиска проблемы

- Тогда изучаем места расположения точек доступа
- И вот она, причина
- Большая часть точек доступа расположена в местах радиотени
- Слабые терминалы просто не могут туда досгучаться

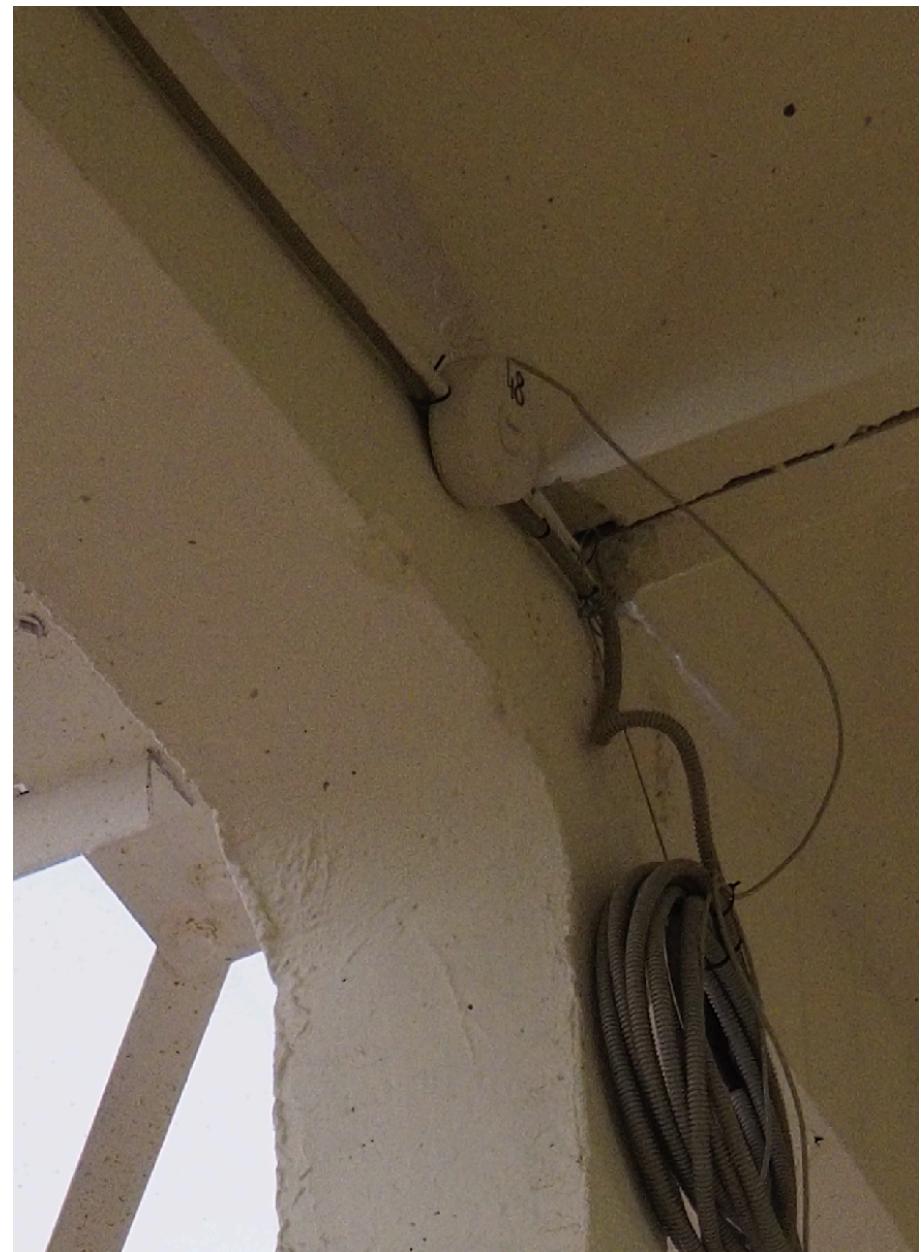
Пример поиска проблемы



Пример поиска проблемы



Пример поиска проблемы



Причины проблем

Ошибки проектирования

- Обычно связаны с:
- Недостаточными знаниями специалиста в физике, распространении радиоволн, антенных и фидерных устройствах
- Неточными данными об планировке объекта
- Неиспользованием специального ПО для проектирования покрытия (Wireless Planner)
- Отсутствием предпроектного обследования

Плохая настройка AP

- Некорректный выбор канала или мощности передатчика
- Некорректный выбор стандартов передачи данных
- Некорректный выбор параметров безопасности

Изменение радиобстановки

- К сожалению беспроводная сеть не ограничивается границами помещения
- У вас может появиться сосед, который активно будет использовать тот же канал, что и вы
- В зоне сети может появиться оборудование создающее помехи на частотах работы WiFi

Целенаправленная атака

- К сожалению беспроводные сети не застрахованы от атак
- Часто атака производится на сам протокол 802.11, например на управляющие фреймы
- Типовой пример Deauth-Attack
- На данный момент появились дешевые устройства в которые возможно установить специализированную прошивку для такой атаки

Целенаправленная атака

- Устройство содержит в себе точку доступа и встроенный web-сервер для настройки
- Питается от micro-USB
- Стоит около 200 рублей



New Wireless module CH340 NodeMcu V3 Lua WiFi Internet of Things development board based ESP8266

Англ. Посмотреть название на русском (автоматический перевод)

★★★★★ 4.9 (1142 голоса(ов)) | 1480 заказа(ов)

Цена: **157,26 руб.** / шт.

Доставка: 61,26 руб. в Russian Federation службой AliExpress Saver Shipping
Расчетное время доставки: 23-32 дн. ?

Количество: - 1 + шт. (59608 шт. Доступно)

Общая стоимость: 218,52 руб.

[Купить сейчас](#) [Добавить в корзину](#)

[Добавить в "Мои желания"](#) (1657 добавили) (

Целенаправленная атака

APs Stations Attacks Settings Info

Scan for Wi-Fi access points

SCAN

Networks found: 9
MAC:

DESELECT ALL SELECT ALL

Ch	SSID	RSSI	Select
1	ikn	-55	SELECT
13	winterdream	-60	SELECT
11	beeline	-71	SELECT
9	Fedor2	-81	SELECT
10	TP-LINK_79CC	-86	SELECT
2	wifi	-89	SELECT
1	Smart_box-50D0FC_guest	-89	SELECT
1	rpolinella	-90	SELECT
5	SXX	-90	SELECT

INFO: You may have to reload the site to see the results.

APs Stations Attacks Settings Info

Attacks

Selected AP(s): CLONE
• ikn

Selected Station(s):
• FF:FF:FF:FF:FF - BROADCAST

Attack	Status	Start/Stop
Deauth	ready	START
Beacon	ready	START
Probe-Request	ready	START

5 0 S ENABLE RANDOM

INFO: You may lose connection when starting the attack.
Change the channel in the settings to the same of the selected AP to prevent this.

Целенаправленная атака

Time (s)	Interf...	Channel	Signal...	Rate	Dst.	Src.	Type	
0.316	wlan1	2412/20...	-57	1Mbps	FF:FF:FF:FF:FF:FF	E4:8D:8C:50:BD:AD	disassocia...	
0.317	wlan1	2412/20...	-55	6Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.317	wlan1	2412/20...	-56	6Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.317	wlan1	2412/20...	-57	2Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.318	wlan1	2412/20...	-57	2Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.318	wlan1	2412/20...	-56	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.319	wlan1	2412/20...	-56	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.319	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.320	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.321	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.321	wlan1	2412/20...	-56	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.322	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	deauthen...	
0.322	wlan1	2412/20...	-56	6Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.322	wlan1	2412/20...	-56	6Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.322	wlan1	2412/20...	-56	2Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.323	wlan1	2412/20...	-56	2Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.323	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.324	wlan1	2412/20...	-58	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.324	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.325	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.326	wlan1	2412/20...	-56	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.326	wlan1	2412/20...	-58	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.327	wlan1	2412/20...	-57	1Mbps	E4:8D:8C:50:BD:AD	FF:FF:FF:FF:FF:FF	disassocia...	
0.327	wlan1	2412/20...	-57	1Mbps	FF:FF:FF:FF:FF:FF	E4:8D:8C:50:BD:AD	deauthen...	

Рекомендации

- Использовать 2-диапазонные точки доступа, так как:
 - Это увеличивает надежность связи в случае проблем с одним из диапазонов
 - 2.4ГГц диапазон перегружен устройствами
 - Увеличивает количество пользователей, которых может обслужить одна точка доступа
 - Ускоряет работу, особенно с внедрением 802.11ac

Рекомендации

- Тщательно подходить к проектированию покрытия сети
- Не забывать о мониторинге сети
- Не надеяйтесь что у вас не будет проблем
- Не стесняться обратиться к специалистам

СПАСИБО
ЗА ВНИМАНИЕ